(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
6 December 2001 (06.12.2001)

PCT

(10) International Publication Number
WO 01/92349 A2

(51) International Patent Classification[7]: C08F 10/00

(21) International Application Number: PCT/US01/17770

(22) International Filing Date: 31 May 2001 (31.05.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/588,109 31 May 2000 (31.05.2000) US

(71) Applicant: @POS.COM, INC [US/US]; 3051 North 1st Street, San Jose, CA 95134 (US).

(72) Inventors: LUNGARO, James, C.; 1493 Brookdale Drive, San Jose, CA 95125 (US). TSO, Susan, W.; 289 Woodruff Way, Milpitas, CA 95035 (US). FERNANDO, Llavanya; 1310 Rimrock Drive, San Jose, CA 95120 (US). LEE, Simon; 48889 Crown Ridge Common, Fremont, CA 94539 (US).

(74) Agents: KAUFMAN, Michael, A._ et al.; Flehr Hohbach Test Albritton & Herbert LLP, Suite 3400, 4 Embarcadero Center, San Francisco, CA 94111-4187 (US).

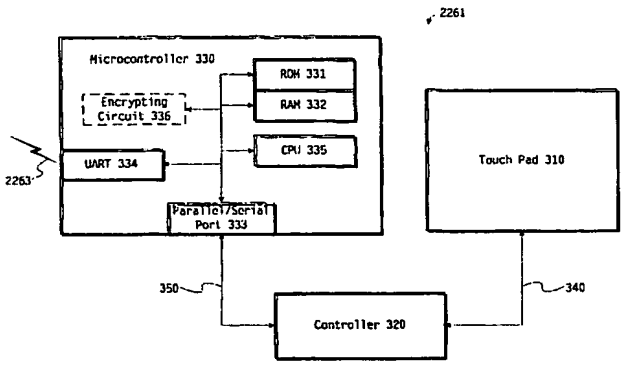
(81) Designated States *(national)*: GB, JP.

(84) Designated States *(regional)*: European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: A SECURE, ENCRYPTING PIN PAD



(57) Abstract: Apparatus and methods for encrypting an identifier such as a PIN entered on a keypad. The apparatus may include a pad, an encrypting circuit adjacent the pad and a link coupling the pad and the encrypting circuit. The pad is for entering an identifier, and the circuit for encrypting the entered identifier. The pad may be a physical touch pad such as an N-wire-technology touch pad. Alternatively, the pad may be a virtual touch screen. The encrypting circuit may be a CPU along with a memory coupled to the CPU and programmed to encrypt. The CPU and programmed memory may be the first CPU programmable to encryp the entered identifier, through which the identifier passes. The encrypting circuit may be a microcontroller programmed to encrypt. In still another variation, the encrypting circuit may be an application-specific integrated circuit (ASIC). The apparatus may include a housing that encloses the encrypting circuit and link. The housing would be resistant to access, tampering or tapping. The housing may be at least partially of chip-on-glass technology. The encrypting circuit may be embedded in the housing, as may the link. A method for encrypting an identifier includes placing a pad for entering an identifier, a circuit for encrypting an identifier and a link communicatively coupling the pad and the circuit adjacent in an access-resistant housing. An identifier is entered on the pad and communicated to the encrypting circuit. The encrypting circuit encrypts the identifier. The encrypted identifier may be forwarded for verification.

WO 01/92349 A2

A SECURE, ENCRYPTING PIN PAD

This invention relates to encryption circuits and to PIN pads. More specifically, this invention relates to the securing through encryption of information entered on a PIN pad.

BACKGROUND

Well established in the art of securing a financial transaction is the use of a key pad to verify that the person transacting business is in fact the rightful person authorized to perform the transaction. Many people are familiar with the personal identification numbers or "PINs" that are ubiquitous in transactions involving debit cards.

The reasoning behind PINs is that only the person authorized to use the account underlying the debit card knows the PIN for the card. As such, any person's ability to produce that PIN on demand verifies that he is in fact the person authorized to transact business using the account.

A weak link in this reasoning is the assumption that knowledge of a PIN proves that the knowledgeable person is the rightful person. A wrongful person of ill will may acquire the PIN through a number of means: She may trick the information from the rightful person. She may oversee the entry of the PIN into a pad. She may access the database of account numbers and PINs of a business that previously completed a transaction with the account. She may access the database of account numbers and PINs of the financial institution maintaining the account. At a more sophisticated level, she may intercept the transmission of the PIN information between the PIN pad on which it is entered and the computer that verifies it.

Figure 1 illustrates a transaction-verification system 100 according to the prior art. The system 100 includes a merchant 120, alliances and partners 130, processing center 140 and service providers 1A0. The system 100 also includes communications links 160, 170 and 180.

The links 160, 180 communicatively couple the merchant 120 and alliances and business partners 130. The links 170, 180 communicatively couple the alliance and partners 130 and the processing center 140. The link 180 communicatively interconnects the merchant 120, the alliances and partners 130, the processing center 140 and the service providers 1A0. The link 180 may be the Internet.

The merchant 120 includes a merchant data center 127, one or more point-of-sale (POS) platforms 126 and the communications link 128. The link 128 communicatively couples the POS system 126 and the merchant data center 127.

The POS platform 126 itself includes a cash register 1262 or the like, a keypad 1261 and a communications link 1263. The link 1263 communicatively couples the cash register 1262 and the keypad 1261.

Where a data center 130, 140, 1A0 verifies a PIN entered on the keypad 1261, the PIN information travels over several of the communications links 1263, 128, 160, 170, 180 before the data center receives the information for verification. A sophisticated malefactor may intercept the PIN information along any of these communications links.

In response, the art has evolved to encrypt or otherwise protect PIN information almost always over a communications link 160, 170 or 180 and sometimes over a communications link 128: The merchant's data center 127 encrypts the PIN before passing it on to the business partner 130, 140, 1A0 to verify.

However, the PIN information still travels unencrypted over multiple communications links. The sophisticated malefactor still may intercept PIN information along the link 1263 between the PIN keypad and the first computer system capable of encrypting the PIN information –

here, the cash register 1262. The sophisticated malefactor may intercept PIN information between the cash register 1262 and the merchant's data center 127.

Accordingly, a method of securing the entry and verification of a PIN is desirable where the unencrypted PIN information virtually cannot be intercepted between its entry on a PIN pad and a first receiving computer system capable of encrypting the information.

These and other goals of the invention will be readily apparent to one of ordinary skill in the art on reading the background above and the description below.

SUMMARY

Herein are described apparatus and methods for encrypting an identifier such as a PIN entered on a keypad. The apparatus may include a pad, an encrypting circuit adjacent the pad and a link. The pad is for entering an identifier, and the circuit for encrypting the entered identifier. The link communicatively couples the pad and the encrypting circuit.

The pad may be a physical touch pad such as an N-wire-technology touch pad (where N is 4, 5, 6, 7 or other). Alternatively, the pad may be a virtual touch screen.

The encrypting circuit may be a CPU along with a memory coupled to the CPU and programmed to encrypt. The CPU and programmed memory may be the first CPU programmable to encrypt the entered identifier, through which the identifier passes.

The encrypting circuit may be a microcontroller programmed to encrypt. In still another variation, the encrypting circuit may be an application-specific integrated circuit (ASIC).

The apparatus may include a housing that encloses the encrypting circuit and link. The housing would be resistant to access,

tampering or tapping. The housing may be at least partially of chip-on-glass technology.

The encrypting circuit may be embedded in the housing, as may the link.

A method for encrypting an identifier includes placing a pad for entering an identifier, a circuit for encrypting an identifier and a link communicatively coupling the pad and the circuit adjacent in an access-resistant housing. An identifier is entered on the pad and communicated to the encrypting circuit. The encrypting circuit encrypts the identifier. The encrypted identifier may be forwarded for verification.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 illustrates a transaction-verification system according to the prior art.

Figure 2 illustrates a transaction system incorporating an embodiment of the invention.

Figure 3 is a block diagram of the components of the keypad from the transaction system of Figure 2.

Figure 4 illustrates physical aspects of the pin pad of Figure 2.

DESCRIPTION OF THE INVENTION

DEVICES

- A Secure, Encrypting PIN Pad

Figure 2 illustrates a transaction-verification system 200 according to the prior art. The system 200 includes a merchant 220, alliances and partners 130, processing center 140 and service providers 1A0. The system 200 also includes communications links 160, 170 and 180.

The links 160, 180 communicatively couple the merchant 220 and alliances and business partners 130. The links 170, 180 communicatively

couple the alliance and partners 130 and the processing center 140. The link 180 communicatively interconnects the merchant 220, the alliances and partners 130, the processing center 140 and the service providers 1A0. The link 180 may be the Internet.

The merchant 220 may include a merchant data center 227, one or more point-of-sale (POS) platforms 226 and the communications link 228. The link 228 communicatively couples the POS system 226 and the merchant data center 227.

The POS platform 226 itself may include a cash register 2262 or the like, a keypad 2261 and a communications link 2263. The link 2263 communicatively couples the cash register 2262 and the keypad 2261.

Figure 3 is a block diagram of the components of the keypad 2261. The keypad 2261 may include a touch-pad 310, a controller 320 and a microcontroller 330, as well as the communications links 340 and 350. The link 340 communicatively couples the touch pad 310 and the controller 320, while the link 350 communicatively couples the controller 320 and the microcontroller 330.

The touch pad 310 is of any type known in the art, and therefore, further description of it is omitted – except to say that in one embodiment, the output of the touch pad 310 is consistent with one of the N-wire technologies known in the art of touch pads and that in another embodiment, the touch pad 310 is an LCD/touch-pad combination also known in the art. (N is 4, 5, 7 or some other number.)

The controller 320 contains sufficient intelligence to accept the output of the touch pad 310 and convert it into input usable by the microcontroller 330. Where the output of the touch-pad 310 is N-wire-technology output (N equals, 4, 5, 7 or other), the controller 320 produces an output representative of a sequence of positions where the touch pad 310 has been touched.

The microcontroller 330 may contain a CPU 335, a memory 331, 332, a touch-pad interface 333 and a POS-system interface 334. The memory

331, 332 of the microcontroller 330 may be programmed to perform the invention as described herein, including receiving, converting and encrypting input from the controller 320. Alternatively, the microcontroller 330 may include an application- specific integrated circuit (ASIC) or other hardware 336 for performing the encryption.

The touch-pad interface 333 may be a parallel/serial conversion port.

The microcontroller 330 may be embedded conceptually, physically or both: The microcontroller 330 may form part of a larger machine of some non-computing type, here, a keypad 2261 or a POS 226. Also, the construction of the keypad 2261 may include chip-on-glass (COG) technology, well known in the art of LCDs, wherein the microcontroller 330 and the touch pad controller 320 are embedded in glass. Where the microcontroller 330 and the controller 320 are embedded, the link 350 may be embedded. Preferably, the link 340 is embedded as much as is practicable.

Alternatively, the microcontroller 330 and the controller 320 may be embedded in the substance of the touch pad 310. That is to say, the circuitry 330, 320 may exist in the glass or the substrate of the touch pad 310 or in the (typically, plastic) housing of the touch pad 310. Again, where the circuitry 330, 320 are embedded, the link 350 may be embedded – preferably, as much as is practicable.

The embedding technology (COG or otherwise) has the advantage that the surrounding mass provides tamper-resistant protection -- particularly anti-tap protection -- for the microcontroller 330 and the circuitry 320 and links 340, 350 between it and the touch pad 310. Also, the adjacency (that is to say, nearness) of the microcontroller 330 to the touch pad 310 reduces the physical space to which a malfeasant may have access.

The touch pad 310 may have a flex tail for its connection 340. The flex tail may be embedded in the glass, substrate or housing of the touch pad 310.

Figure 4 illustrates physical aspects of the pin pad 2261. The glass 370 and the touch pad 310 touch. The circuit 330 is sandwiched between the glass 370 and the touch pad 310. The glass is less than 0.5 inches thick and is typically 0.053 inches or less.

When a person touches the keypad, an N-wire-technology touch pad 310 generates voltages. The controller 320 converts these voltages into positional representations ("positions") and presents these positions to the microcontroller 330 on the interface 333. The microcontroller 330 converts the representations from positional to alphanumeric.

Now, with the alphanumeric PIN in its memory 331, 332, the microcontroller 330 encrypts the PIN information and forwards it to the verifying component (say, transaction-security component 1A0) of the transaction system for verification.

As is well known in the art of encryption, at least one component of the transaction system 200 knows how to decrypt the PIN information from the keypad 2261. However, some component different from the verifying component and between the keypad 2261 and the verifying component may decrypt the PIN information and re-encrypt it according to a second protocol before forwarding it to the verifying component. Alternatively, an intermediate component may doubly encrypt the PIN information, that is to say, encrypt the already encrypted PIN information (possibly according to a second protocol) before forwarding that information to the verifying component.

The invention now being fully described, many changes and modifications that can be made thereto without departing from the spirit or scope of the appended claims will be apparent to one of ordinary skill in the art. The controller 320's converting the positional information of the touch pad 310 into alphanumeric information (rather than the

microcontroller's doing so) is an example. That the circuit 330 may be separate or integrated into the touch pad is another example.

WHAT IS CLAIMED IS:

1. An apparatus for encrypting an identifier, the apparatus comprising:

a pad for entering an identifier;

a circuit, adjacent the pad, for encrypting the entered identifier; and

a link, communicatively coupling the pad and the encrypting circuit.

2. The apparatus of claim 1, wherein the pad comprises

a touch pad.

3. The apparatus of claim 2, wherein the touch pad comprises

an N-wire-technology touch pad.

4. The apparatus of claim 2, wherein the touch pad comprises

a four-wire-technology touch pad.

5. The apparatus of claim 2, wherein the touch pad comprises

a seven-wire-technology touch pad.

6. The apparatus of claim 1, wherein the pad comprises

a touch screen.

7. The apparatus of claim 1,

wherein the pad comprises

a pad for entering a personal identifier (PIN).

8. The apparatus of claim 1, wherein the encrypting circuit comprises

a CPU; and

a memory, coupled to the CPU and programmed to encrypt.

9. The apparatus of claim 8, wherein the CPU and programmed memory are the first CPU, programmable to encrypt the entered identifier, through which the identifier passes.

10. The apparatus of claim 1, wherein the encrypting circuit comprises

a microcontroller programmed to encrypt.

11. The apparatus of claim 1, wherein the encrypting circuit comprises

an application-specific integrated circuit (ASIC).

12. The apparatus of claim 1, further comprising

a housing enclosing the encrypting circuit and link and resistant to access.

13. The apparatus of claim 12, wherein the housing comprises housing resistant to tampering.

14. The apparatus of claim 12, wherein the housing comprises housing resistant to tapping.

15. The apparatus of claim 12, wherein the housing comprises

housing at least partially of chip-on-glass technology.

16. The apparatus of claim 12, wherein the housing comprises housing in which the encrypting circuit is embedded.

17. The apparatus of claim 12, wherein the housing comprises housing in which the link and encrypting circuit are embedded.

18. An apparatus for encrypting an identifier, the apparatus comprising:

a pad, comprising one of a touch screen and an N-wire-technology touch pad, for entering a personal identifier (PIN);

a circuit, adjacent the pad and comprising one of a programmed microcontroller and an ASIC, for encrypting the entered identifier;

a link, communicatively coupling the pad and the encrypting circuit; and

a housing, resistant to access and at least partially of chip-on-glass technology, in which the link and encrypting circuit are embedded.

19. A method for encrypting an identifier, the method comprising:

placing a

pad for entering an identifier,

a circuit for encrypting an identifier and

a link communicatively coupling the pad and the encrypting circuit

adjacent in an access-resistant housing;

entering a identifier on the pad;

communicating the identifier to the encrypting circuit; and

encrypting the identifier by means of the encrypting circuit.

20. The method of claim 19, further comprising the step of forwarding the encrypted identifier for verification.

21. An apparatus for encrypting an identifier, the apparatus comprising:

a pad for entering an identifier;

a circuit for encrypting the entered identifier, the circuit being the first circuit receiving and programmable or designed to encrypt the entered identifier;

a link, communicatively coupling the pad and the encrypting circuit; and

a housing, shielding the link and circuit from physical access.

22. The apparatus of claim 21, wherein the circuit comprises

a circuit adjacent the pad.

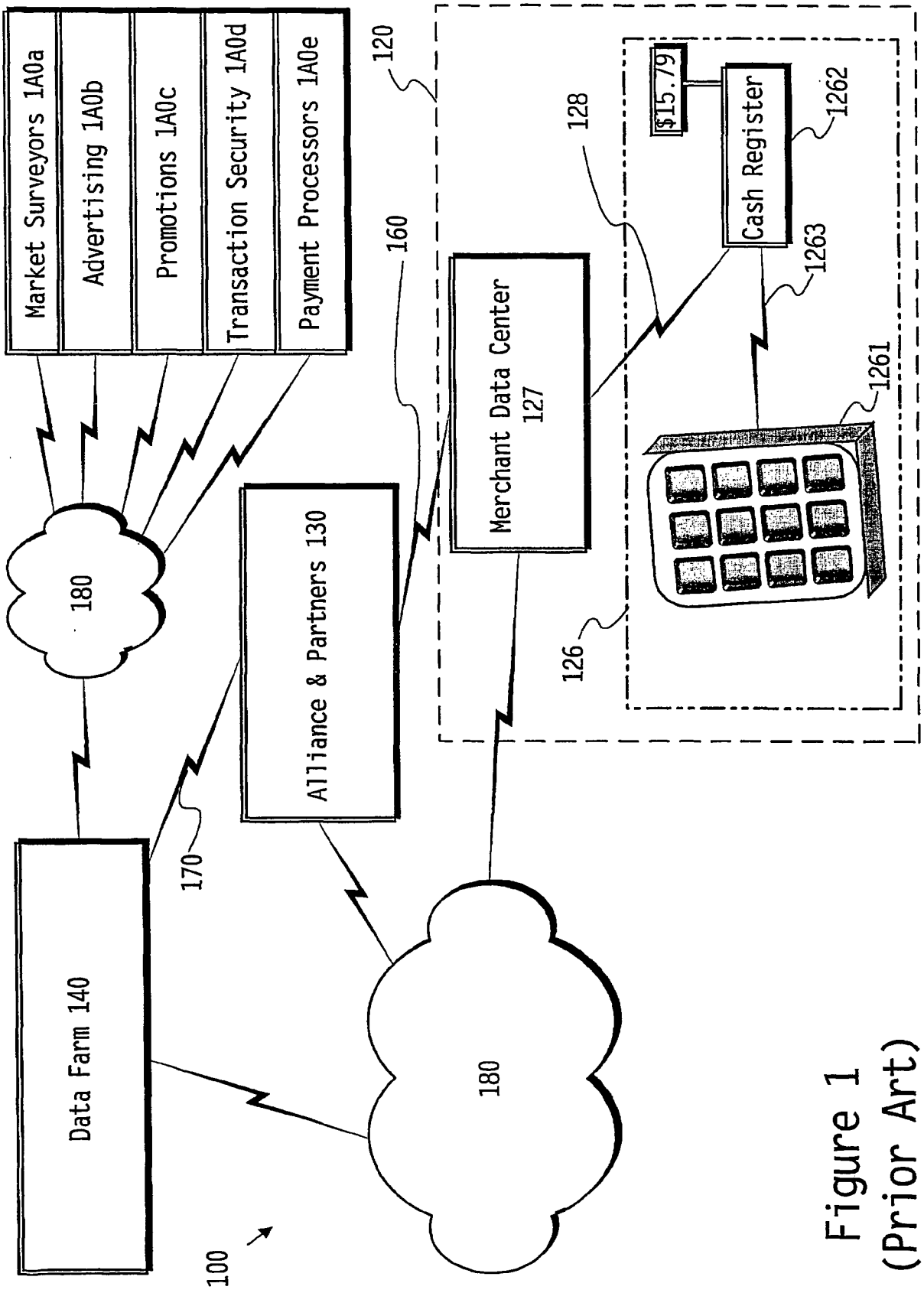


Figure 1
(Prior Art)

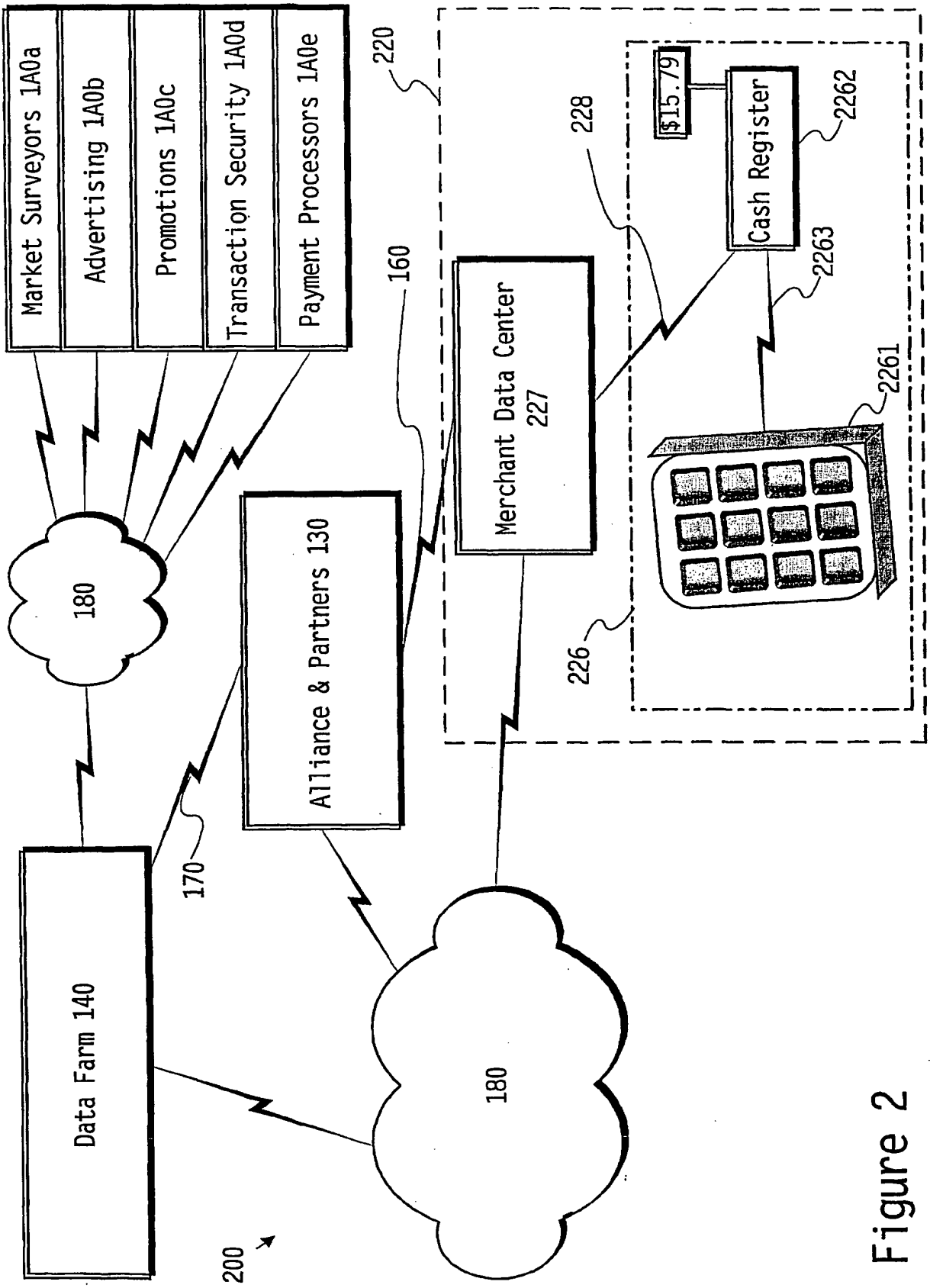

Market Surveyors 1A0a
Advertising 1A0b
Promotions 1A0c
Transaction Security 1A0d
Payment Processors 1A0e
220
228
$15.79
Cash Register
2262
2263
2261
160
Merchant Data Center
227
180
Alliance & Partners 130
226
170
Data Farm 140
180
200

Figure 2

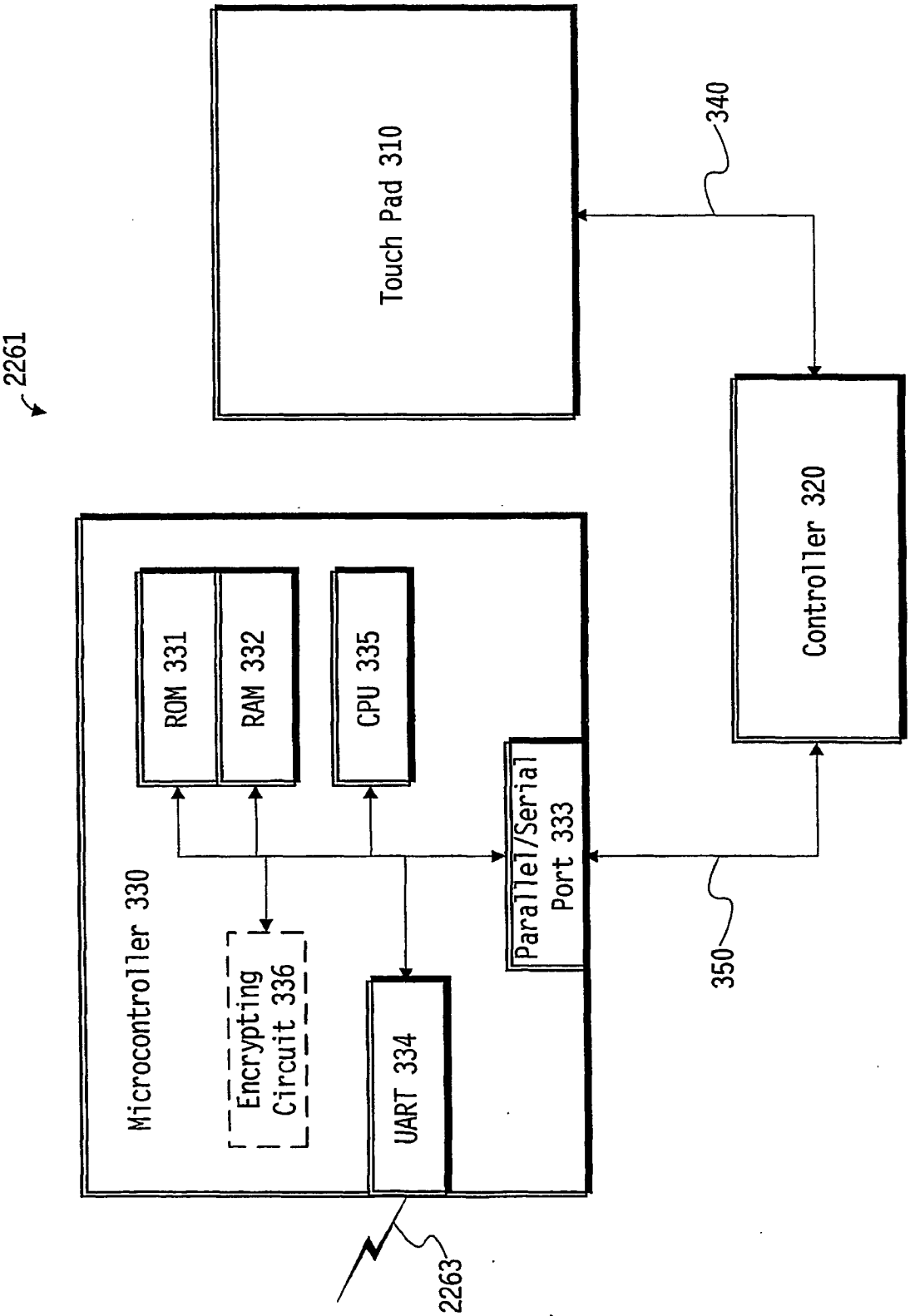

2261
Touch Pad 310
340
Controller 320
ROM 331
RAM 332
CPU 335
Parallel/Serial Port 333
Microcontroller 330
Encrypting Circuit 336
UART 334
350
2263

Figure 3

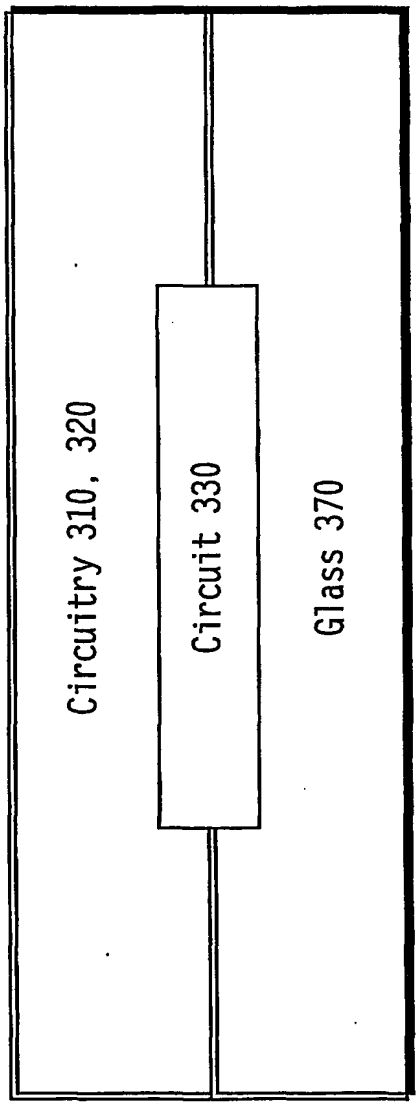


Figure 4

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
6 December 2001 (06.12.2001)

PCT

(10) International Publication Number
WO 01/092349 A3

(51) International Patent Classification[7]: G07F 7/10, G07C 9/00, G07F 19/00, 1/00

(21) International Application Number: PCT/US01/17770

(22) International Filing Date: 31 May 2001 (31.05.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/588,109 31 May 2000 (31.05.2000) US

(71) Applicant: **@POS.COM, INC** [US/US]; 3051 North 1st Street, San Jose, CA 95134 (US).

(72) Inventors: **LUNGARO, James, C.**; 1493 Brookdale Drive, San Jose, CA 95125 (US). **TSO, Susan, W.**; 289 Woodruff Way, Milpitas, CA 95035 (US). **FERNANDO, Llavanya**; 1310 Rimrock Drive, San Jose, CA 95120 (US). **LEE, Simon**; 48889 Crown Ridge Common, Fremont, CA 94539 (US).

(74) Agents: **KAUFMAN, Michael, A.** et al.; Flehr Hohbach Test Albritton & Herbert LLP, Suite 3400, 4 Embarcadero Center, San Francisco, CA 94111-4187 (US).

(81) Designated States *(national)*: GB, JP.

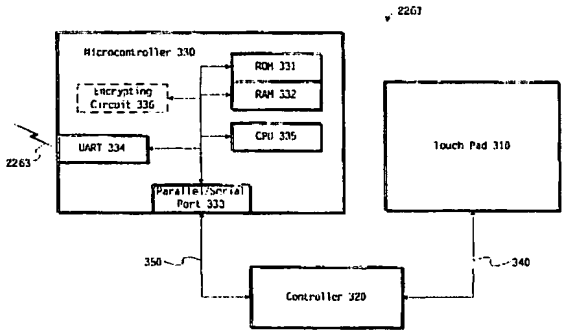
(84) Designated States *(regional)*: European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

Published:
— *with international search report*

(88) Date of publication of the international search report:
17 October 2002

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: A SECURE, ENCRYPTING PIN PAD



(57) Abstract: Apparatus and methods for encrypting an identifier such as a PIN entered on a keypad. The apparatus may include a pad, an encrypting circuit adjacent the pad and a link coupling the pad and the encrypting circuit. The pad is for entering an identifier, and the circuit for encrypting the entered identifier. The pad may be a physical touch pad such as an N-wire-technology touch pad. Alternatively, the pad may be a virtual touch screen. The encrypting circuit may be a CPU along with a memory coupled to the CPU and programmed to encrypt. The CPU and programmed memory may be the first CPU programmable to encryp the entered identifier, through which the identifier passes. The encrypting circuit may be a microcontroller programmed to encrypt. In still another variation, the encrypting circuit may be an application-specific integrated circuit (ASIC). The apparatus may include a housing that encloses the encrypting circuit and link. The housing would be resistant to access, tampering or tapping. The housing may be at least partially of chip-on-glass technology. The encrypting circuit may be embedded in the housing, as may the link. A method for encrypting an identifier includes placing a pad for entering an identifier, a circuit for encrypting an identifier and a link communicatively coupling the pad and the circuit adjacent in an access-resistant housing. An identifier is entered on the pad and communicated to the encrypting circuit. The encrypting circuit encrypts the identifier. The encrypted identifier may be forwarded for verification.

WO 01/092349 A3

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 01/17770

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G07F7/10 G07C9/00 G07F19/00 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G07F G07C G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0 809 171 A (SCHLUMBERGER TECHNOLOGIES) 26 November 1997 (1997-11-26)	1,2, 6-10, 12-14, 16,17, 19-22
A	abstract; figures 1,4 column 4, line 15 -column 5, line 18 column 6, line 40 -column 7, line 37 column 16, line 32 - line 52	3,5,11, 15,18
X	WO 98 14915 A (OMEGA DIGITAL DATA) 9 April 1998 (1998-04-09)	1,7-9, 12,13, 19-22
A	abstract; claims; figures 3-5 page 8, line 10 -page 9, line 13	10,18

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
11 June 2002	25/06/2002

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	David, J

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 01/17770

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
X	WO 98 12615 A (TRANSACTION TECHNOLOGY) 26 March 1998 (1998-03-26)	1,2, 6-10, 12-14, 19-22
A	abstract; claims; figures page 7, line 6 -page 11, line 18	15-18
A	WO 00 17758 A (Y. REDLER) 30 March 2000 (2000-03-30)	
A	EP 0 388 571 A (AMPER) 26 September 1990 (1990-09-26)	
A	EP 0 248 712 A (ÉLECTRONIQUE SERGE DASSAULT) 9 December 1987 (1987-12-09)	
A	G.G. PAPAS: "ENCRYPTION PIN PAD" IBM TECHNICAL DISCLOSURE BULLETIN, vol. 26, no. 5, October 1983 (1983-10), pages 2393-2397, XP002201871	

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/US 01/17770

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
EP 0809171	A	26-11-1997	US	5832206 A	03-11-1998
			CA	2197027 A1	26-09-1997
			EP	0809171 A1	26-11-1997
			ZA	9701313 A	23-06-1998
WO 9814915	A	09-04-1998	AU	4447497 A	24-04-1998
			CA	2239009 A1	09-04-1998
			WO	9814915 A2	09-04-1998
			ZA	9708778 A	27-03-1998
WO 9812615	A	26-03-1998	US	5768386 A	16-06-1998
			AU	2111397 A	05-01-1998
			AU	728108 B2	04-01-2001
			AU	6349198 A	14-04-1998
			BR	9710169 A	08-01-2002
			WO	9745781 A2	04-12-1997
			WO	9812615 A2	26-03-1998
			ZA	9701895 A	07-09-1998
WO 0017758	A	30-03-2000	AU	5881799 A	10-04-2000
			WO	0017758 A1	30-03-2000
EP 0388571	A	26-09-1990	ES	2011538 A6	16-01-1990
			DE	388571 T1	11-04-1991
			EP	0388571 A1	26-09-1990
			GR	91300040 T1	15-11-1991
EP 0248712	A	09-12-1987	FR	2599525 A1	04-12-1987
			DE	3774000 D1	28-11-1991
			EP	0248712 A1	09-12-1987
			ES	2023100 T3	01-06-1992
			NO	872257 A	03-12-1987